



Homeland
Security

Daily Open Source Infrastructure Report

26 September 2012

Top Stories

- A corroded pipe that failed and triggered a leak and massive fire at Chevron Corp.'s Richmond, California refinery had a low silicon content that went undetected during tests and therefore was unaddressed. – *Associated Press* (See item [1](#))
- Sunland Inc. of Portales, New Mexico, whose peanut butter was linked to a multi-State Salmonella outbreak, recalled all of the almond and peanut butter products it has manufactured since May. – *Food Safety News* (See item [22](#))
- Researchers from Security Explorations claimed to identify a flaw that affects all Oracle Java SE versions and the billions of devices on which the software is currently installed. – *Softpedia* (See item [39](#))
- A Romanian computer programmer claims to have found a log on the Institute of Electrical and Electronics Engineers's FTP servers containing log-in information for almost 100,000 members. Membership includes top people from fields such as nanotechnology, IT, telecommunications, energy, and biomedical and healthcare. – *Nextgov* (See item [41](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
 - [National Monuments and Icons](#)
-

Energy Sector

1. *September 24, Associated Press* – (California) **Chevron: Failed pipe had unknown weakness.** A corroded pipe that failed and triggered a leak and massive fire at Chevron Corp.'s Richmond, California refinery had a low silicon content that went undetected during the company's tests and therefore was unaddressed, the manager in charge of the facility said September 24. The general manager of Chevron Richmond described the chemical composition of the decades-old, 8-inch pipe section as a contributing factor to the August 6 blaze that sent thousands of people to the hospital with smoke-related complaints and knocked offline one of the nation's largest refineries. He told reporters during a news conference and residents at a community meeting that the company now thinks the pipe was more susceptible to thinning when exposed to high temperatures, a weakness not fully understood or acted upon before the corroded conduit exploded. The manager said the section that failed was part of a larger 200-foot-long pipe that was inspected in June at 19 points.

Source: <http://ktar.com/23/1565975/Chevron-Failed-pipe-had-unknown-weakness>

For more stories, see items [16](#), [18](#), [29](#), [41](#), and [47](#)

[\[Return to top\]](#)

Chemical Industry Sector

2. *September 25, WTOV 9 Steubenville* – (West Virginia) **Train derails in Wetzel Co.; about 3 tons of lye pellets spilled.** About 3 tons of sodium hydroxide (lye) pellets spilled after a CSX train derailment that left part of State Route 2 near Proctor, West Virginia, closed for a short time September 25. The road was closed only as a precautionary measure and officials stressed there was no environmental hazard. There was extensive damage to several cars and the rail tracks, but none of the chlorine or other cars were penetrated, said the New Martinsville fire chief. Five rail cars were on their sides off of the track and seven cars derailed but remained upright off the tracks after the incident. Between 2 1/2-3 tons of lye pellets spilled from the damaged rail car that was carrying 132 tons, the New Martinsville fire chief said. He said investigators believe the rail cars were coming from the PPG Plant in Natrium and headed south to the Brooklyn switch yard in the southern end of New Martinsville.
Source: <http://www.wtov9.com/news/news/train-derails-wetzel-co-about-3-tons-sodium-chloride/nSLF4/>
3. *September 24, KQTV 2 St. Joseph* – (Missouri) **EPA fines Boehringer Ingelheim for mercury handling violation.** An animal health company in St. Joseph, Missouri, faces a fine of more than \$68,000 for mishandling mercury waste, KQTV 2 St. Joseph reported September 24. Boehringer Ingelheim must also build a \$300,000 state-of-the-art hazardous waste storage facility as part of its agreement with the U.S. Environmental Protection Agency. Agency inspectors found several violations at the facility in 2010. The violations include storing mercury without a permit, sending mercury waste to a non-authorized facility, and transporting hazardous waste without a

license. Boehringer uses mercury as part of its vaccine production process.

Source: http://stjoechannel.com/fulltext?nxd_id=299962

4. *September 24, WCBD 2 Charleston* – (South Carolina) **Authorities investigate cause of Monday explosion at MeadWestvaco Plant in North Charleston.** Fire crews spent about 3.5 hours dealing with an explosion and fire at the MeadWestvaco Corporation chemical plant in North Charleston, South Carolina, September 24. A North Charleston Fire Department spokeswoman said it appeared a 250,000-gallon tank of crude oil ruptured. Firefighters from the facility, North Charleston, Charleston, and St. Andrews fire departments were on scene along with South Carolina Department of Health and Environmental Control units. There was a minor explosion and fire at the facility and one person was transported to a hospital, company officials said. There is no risk to the outside community, they said. Truck drivers outside the plant had to wait hours to move their cargo onto the property.

Source: <http://www2.counton2.com/news/2012/sep/24/11/hazmat-crews-respond-possible-explosion-paper-mill-ar-4614433/>

For another story, see item [15](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

5. *September 25, WECT 6 Wilmington* – (North Carolina) **GE Hitachi's GLE receives license to build laser enrichment facility.** GE Hitachi's Global Laser Enrichment (GLE) announced September 25 the receipt of its license from the U.S. Nuclear Regulatory Commission (NRC) to build a first-of-its-kind laser uranium enrichment facility in Wilmington, North Carolina. The new license will allow the plant to produce up to six million single work units per year, according to a press release. While the license to have the facility was approved, the next step in the process is for the company to make a commercialization decision.

Source: <http://www.wect.com/story/19634063/ge-recieve-license-to-build-laser-enrichment-facility>

6. *September 24, Nuclear Power International* – (Florida) **Regulators approve uprate project for Florida nuclear power plant.** The Nuclear Regulatory Commission (NRC) September 24 approved a power uprate request by Florida Power & Light (FP&L) to increase the power output of the St. Lucie, Florida nuclear power plant's Unit 2 reactor by 17 percent, from approximately 853 to 1,002 MWe. A similar uprate was approved July 9 for the Port St. Lucie plant's Unit 1. The NRC staff's evaluation determined that FP&L could safely increase the reactor's power output primarily by carrying out upgrades to several plant systems and components, including the steam and power conversion system and the condensate and feedwater system. FP&L intends to implement the uprate in the next few months.

Source: <http://www.power-eng.com/articles/2012/09/regulators-approve-uprate-project-for-florida-nuclear-power-plant.html>

[\[Return to top\]](#)

Critical Manufacturing Sector

Nothing to report

[\[Return to top\]](#)

Defense Industrial Base Sector

7. *September 24, Threatpost* – (International) **Another IE exploit targeting defense industry discovered.** Another malicious Web site was discovered hosting an exploit for the zero-day vulnerability Internet Explorer patched by Microsoft the week of September 17. This site, like the other exploits discovered, targets the defense and space industries, and is dropping an unknown payload, according to Barracuda Labs. One researcher said the compromised site is not likely a drive-by attack, but instead may be included in phishing email messages to specific individuals within those respective industries. Previous exploits were dropping either the Poison Ivy or PlugX remote access trojans. This malicious file discovered by Barracuda has a similar file name to the others, Grumgog.swf, named after a character in a video game. Barracuda did not identify the payload dropped here, but did call it a backdoor.

Source: http://threatpost.com/en_us/blogs/another-ie-exploit-targeting-defense-industry-discovered-092412

[\[Return to top\]](#)

Banking and Finance Sector

8. *September 25, Softpedia* – (New Hampshire; International) **JPMorgan Chase Bank servers hacked, Tiffany employee details exposed.** Computer servers owned by JPMorgan Chase Bank were breached, and the financial institution alerted high-end jewelry company Tiffany & Co because the affected machines contained the personal details of some employees, Softpedia reported September 25. “Chase told us that the affected servers, which contained certain information provided in connection with a Tiffany employee travel expense reimbursement system, contained information such as names, addresses, Social Security numbers and banking information,” Tiffany’s chief privacy officer wrote in a letter September 5 to the New Hampshire attorney general. The bank told the company it had no reason to believe that the sensitive data has been copied or misused by the attackers. The financial institution also shut down the affected servers and upgraded its security systems to prevent such incidents from occurring in the future. Tiffany also sent out letters to the impacted individuals – there are “approximately” three employees from New Hampshire – advising them to be on the lookout for any suspicious transactions.

Source: <http://news.softpedia.com/news/JPMorgan-Chase-Bank-Server-Hacked-Tiffany-Employee-Details-Exposed-294557.shtml>

9. *September 25, Softpedia* – (International) **Bank of America website reveals details of random users, experts find.** While logging in to Bank of America's (BoA) Web site to access the Automated Clearing House (ACH) system, experts from Private Internet Access noticed they were actually viewing the bank account details of some other random customer, Softpedia reported September 25. After they entered the transfer interface, they were presented with the name, bank account, balance, email address, and other details of an individual who had nothing to do with the company. Apparently, the account is restored to normal after the user logs out and logs back in again, and the security hole could not be reproduced after this first occurrence. However, some users reported that they also encountered the problem in the past, which meant that it was not an isolated incident. Private Internet Access representatives made screenshots and sent out a detailed notification to BoA.
Source: <http://news.softpedia.com/news/Bank-of-America-Website-Reveals-Details-of-Random-Users-Experts-Find-294534.shtml>
10. *September 25, Philadelphia Inquirer* – (National) **Discover to pay \$214 million to settle charges of deceptive marketing.** More than 3.5 million people who used Discover credit cards over the last 5 years will share about \$200 million in restitution for marketing practices that federal regulators said were unfair and deceptive, the Consumer Financial Protection Bureau and the Federal Deposit Insurance Corporation announced September 24. The compensation will go to customers charged for add-on products such as "Payment Protection" or "Wallet Protection." Regulators said telemarketers for the Delaware bank followed misleading scripts and often sped through fee disclosures, leading customers to believe that the bank was touting benefits that came free with their cards. Discover also agreed to pay \$14 million in penalties to settle the case. About 4.7 million customers were billed for the services between December 2007 and August 2011, the period covered by the case.
Source: http://www.philly.com/philly/business/20120925_Discover_to_pay_214_million_to_settle_charges_of_deceptive_marketing.html
11. *September 25, Wall Street Journal* – (International) **Treasury targets Sinaloa operative and his associates.** The U.S. Department of the Treasury said September 25 that it placed Kingpin Act sanctions on an associate of the head of the Sinaloa Cartel, and four of his collaborators. The man is the head of a narcotics distribution and money laundering organization based in Guadalajara and Mexico City, Mexico, Treasury said. The man was arrested in March 2011 as part of a sweep by law enforcement in Mexico and Ecuador that netted several members of his organization. More members of the network were arrested in July 2011. The United States is seeking his and his associates' extradition to face charges in a May 2011 indictment that alleges drug-trafficking and money laundering offenses. The indictment arose out of a U.S. Drug Enforcement Administration probe that linked his organization to the movement of cocaine by the ton in Ecuador and Mexico, and the laundering of millions of U.S. and Canadian dollars through the international financial system.
Source: <http://blogs.wsj.com/corruption-currents/2012/09/25/treasury-targets-sinaloa-operative-and-his-associates/>

12. *September 24, KPRC 2 Houston* – (Texas) **Police: Bank robber sprays employees with chemicals.** A man sprayed bank employees with a chemical believed to be pepper spray during an armed robbery in Shenandoah, Texas, September 24, police said. Shenandoah police said a man walked into a Citibank branch, pulled a small-framed semi-automatic rifle from his backpack, and walked up to a teller. The man demanded cash and sprayed the teller. There was one customer in the bank at the time of the robbery who was also sprayed. Police said the robber then went from office to office and sprayed other employees. Some workers were able to close their doors and avoid the substance. The man went back to the teller he attacked and then demanded cash. The people who were sprayed with the chemicals were treated at the scene. Hazardous materials crews cleared the air inside.
Source: <http://www.click2houston.com/news/Police-Bank-robber-sprays-employees-with-chemicals/-/1735978/16719986/-/hk8to4/-/index.html>
13. *September 24, Help Net Security* – (International) **Stolen card data on sale on professional-looking e-shop.** A researcher from Webroot recently uncovered a seemingly well-established Web site for selling stolen card data, so much so that the crook behind the scheme has set up a professional-looking e-shop. The shop is advertised on a number of carding forums, and the crook can be contacted only via ICQ. The page is well designed and features a shop whose functionality does not seem to differ much from any other legitimate one. The e-shop also has a helpful search engine so customers can find exactly what they need. “The service is currently offering 9,132 stolen credit cards for sale, and has already managed to sell 3,292 credit cards to prospective cybercriminals,” the researcher said, noting that the going rate for a sample stolen credit card depends on whether the card is debit or credit. The former go for \$16, and the latter for \$30 per item, but there are also discounts to be had for bulk purchases. Rather than exploiting the stolen card numbers, services like the e-shop forward the risk on to those who purchase the numbers and then attempt to exploit them.
Source: <http://www.net-security.org/secworld.php?id=13652>

For another story, see item [46](#)

[\[Return to top\]](#)

Transportation Sector

14. *September 25, Associated Press* – (Virginia) **Airports authority: Bomb threat delayed arriving flights at DC-area airport; nothing found.** Officials said an investigation into a bomb threat at Washington Dulles International Airport in Dulles, Virginia, September 24 delayed several arriving flights, but no bomb was found. A Metropolitan Washington Airports Authority spokeswoman said authorities investigated two parking garages that were closed to the public for several hours. Delays affected flights scheduled to arrive between 8:30 p.m. and 9 p.m. Flights were back to normal.
Source: http://www.washingtonpost.com/local/airports-authority-bomb-threat-delayed-arriving-flights-at-dc-area-airport-nothing-found/2012/09/25/066fbf22-06fa-11e2-9eea-333857f6a7bd_story.html

15. *September 25, WSMV 4 Nashville* – (Tennessee) **I-24 reopens after sulfuric acid spill.** Interstate 24 East in downtown Nashville, Tennessee, reopened September 25 after a sulfuric acid spill closed the roadway for about 12 hours. The spill was reported near exit 48 at James Robertson Parkway in east Nashville. The ramp to James Robertson Parkway would remain closed indefinitely, officials indicated. They said they believed a tanker may have leaked the chemical from Clarksville to Nashville. Clarksville police said that a sulfuric acid spill was also reported near the Nyrstar plant, located near Zinc Plant Road and Cumberland Drive.
Source: <http://www.wsmv.com/story/19628115/wreck-hazardous-spill-closes-eastbound-i-24>
16. *September 25, Sheridan Media* – (Wyoming) **Oil tanker crash closes I-25.** The Wyoming Highway Patrol announced Interstate 25 was closed due to an oil tanker crash, Sheridan Media reported September 25. Troopers estimate approximately 200 barrels of crude oil and cargo spilled on the highway because the tanker was breached during the crash. Northbound traffic was diverted onto WYO 320 at Wheatland and southbound traffic was diverted at the US 26 Junction. The tractor trailer combination is owned by Basin Western Incorporated out of Roosevelt, Utah.
Source: <http://www.sheridanmedia.com/news/oil-tanker-crash-closes-i-2552987>
17. *September 25, Anchorage Daily News* – (Alaska) **Kenai River's neighbors brace for high water.** The latest round of widespread flooding to hit southcentral Alaska is aimed at the Kenai Peninsula, the Anchorage Daily News reported September 25. The National Weather Service extended a flood warning for the Kenai River until September 27. At Cooper Landing, the Kenai River was at moderate flood stage September 24. The weather service said that the river would likely continue to rise below Skilak Lake. The Alaska Department of Natural Resources (DNR) closed the Kenai River to boat traffic September 24 because of dangerously high water. It was only the second time in the history of the river management area that a director has ordered such a closure, said a DNR spokeswoman. In the Matanuska-Susitna Borough, three full structures were lost and there were 14 road closures. In Talkeetna, residents were advised to boil their water for at least 2 minutes while crews continue to test whether it is safe. In Seward, crews were working to stabilize the Lowell Creek Bridge and clear landslides from Lowell Point Road that have cut off the community. Water taxis were transporting Lowell Point residents to and from the Seward harbor. A portion of taxiway at the Girdwood Airport was damaged when water topped Crow Creek near the airport, said a department of transportation spokesman, but the airport was open and operational. Track washouts and lost revenue likely will cost the Alaska Railroad more than \$1 million, a railroad spokeswoman said. About 500 feet of mainline track were left dangling September 22 near Gold Creek. The spokeswoman said the main line could open as early as September 26. Trains between Anchorage and Fairbanks were not operating since September 19.
18. *September 25, Detroit Free Press* – (Michigan) **Semis crash in Novi, Taylor within hours of fuel tanker clean-up.** Semi-trucks crashed along Michigan highways in Taylor and Novi September 25, within about an hour of I-696 in Farmington Hills

reopening after a fuel truck crashed there September 24. A Michigan State Police lieutenant said a semi crashed on I-96 in Novi early the afternoon of September 25. Another semi crashed on the ramp from northbound Telegraph to eastbound I-94, according to a Taylor police sergeant. He estimated the ramp would be closed for about 3 hours. The crashes came just after eastbound I-696 between I-275 and Orchard Lake reopened about 20 hours after a fuel truck carrying 10,000 pounds of gasoline — or about 1,600 gallons — crashed after being cut off by a car, according to Michigan State Police. The driver suffered minor head and back injuries. The section of freeway was closed overnight and for a few hours September 25 for crews to remove the fuel and semi from the ditch.

Source: <http://www.freep.com/article/20120925/NEWS05/120925010/Eastbound-I-696-to-reopen-for-rush-hour-after-overtuned-gas-tanker-shuts-stretch>

19. *September 24, Kenewick Tri-City Herald* – (Oregon) **Chemical bomb scare closes Highway 395 near Stanfield, Ore.** A chemical bomb scare closed a section of Oregon’s Highway 395 near Stanfield September 23. Stanfield police stopped a vehicle for a traffic infraction and the investigation reportedly revealed “chemicals and materials not typically transported inside the cab of a vehicle, which caused the officer concern,” said the Stanfield police chief in a release. A man reportedly told the officer he was attempting to make a chemical bomb to blow up a large area. Emergency officials closed Highway 395 from Interstate 84 to South Edwards Road. The chemicals inside the vehicle appeared to be household chemicals available for purchase at most hardware stores. The suspect was jailed on suspicion for possessing a controlled substance, methamphetamine, first-degree disorderly conduct, and attempted unlawful manufacture of a destructive device.

Source: <http://www.tri-cityherald.com/2012/09/24/2113135/chemical-bomb-scare-closes-highway.html>

For more stories, see items [2](#) and [7](#)

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report

[\[Return to top\]](#)

Agriculture and Food Sector

20. *September 25, Associated Press* – (Georgia) **Feds offer drought aid in 6 more Georgia counties.** The U.S. Small Business Administration (SBA) extended its disaster loan program to six more Georgia counties affected by drought, the Associated Press reported September 25. The loans target farm-related and other entities not covered by aid from the U.S. Department of Agriculture. The newly eligible counties are Bartow, Chattooga, Floyd, Gordon, Polk, and Walker. In August, SBA declared 12 other counties eligible for aid.

Source: <http://www.cbsatlanta.com/story/19632029/feds-offer-drought-aid-in-6-more-georgia-counties>

21. *September 24, U.S. Food and Drug Administration* – (National) **Hanover Pike Enterprises, Inc issues allergy alert on undeclared margarine containing milk and soy in jams and jellies.** According to a September 24 release by the U.S. Food and Drug Administration, Hanover Pike Enterprises, Inc. of Hampstead, Maryland, notified customers that its 8-ounce and 4-ounce jars of Hot Pepper Jelly and Green Pepper Jelly and its 4-ounce and 9-ounce jars of Blackberry Brandy Jam and Peach Brandy Jam may contain undeclared milk and soy. These items were distributed nationwide through retail stores and via the company Web site under the label “Jill’s Jams Mixes and More” or “Jill’s Jams and Jellies.” This notification was initiated after it was discovered the products containing milk and soy were distributed in packaging that did not list milk or soy as ingredients.

Source: <http://www.fda.gov/Safety/Recalls/ucm320677.htm>

22. *September 24, Food Safety News* – (National) **Peanut butter recall expands beyond Trader Joe’s.** Sunland Inc. of Portales, New Mexico, whose peanut butter was linked to a multi-State Salmonella outbreak, issued a massive recall of products September 24. The company recalled all almond butter and peanut butter products manufactured since May because they may be contaminated with Salmonella Bredeney, a rare strain of Salmonella that has caused at least 29 illnesses in 18 States since June 11. This large market withdrawal follows a more limited one initiated by Trader Joe’s September 21, which included its Valencia Creamy Salted Peanut Butter. All affected products bear a best-if-used-by date between May 1, 2013 and September 24, 2013.

Source: <http://www.foodsafetynews.com/2012/09/peanut-butter-recall-expands-beyond-trader-joes/#.UGDD-ZH2q70>

23. *September 24, Peninsula Daily News* – (Washington) **Seven persons hospitalized after eating toxic Discovery Bay mussels.** Seven vacationing family members were hospitalized, one so severely that she was placed on a ventilator, after eating mussels tainted with a potentially deadly marine biotoxin that they harvested from Discovery Bay in Washington the weekend of September 22, health officials said. Jefferson County Public Health said family members fell ill with paralytic shellfish poisoning, or PSP. Discovery Bay has been closed to recreational shellfish harvesting for high levels of PSP since mid-July. Most beaches on the North Olympic Peninsula remain closed to recreational shellfish harvesting because of high levels of PSP toxin. Fisheries that remain closed for PSP are Discovery Bay, Admiralty Inlet, Port Townsend Bay, Kilsut Harbor, including Mystery Bay, Oak Bay, Mats Mats Bay, and Port Ludlow south to the Hood Canal Bridge. All Clallam County beaches remain closed for recreational shellfish harvesting for unsafe levels of PSP.

Source:

<http://www.peninsuladailynews.com/article/20120925/NEWS/309259996/seven-persons-hospitalized-after-eating-toxic-discovery-bay-mussels>

24. *September 24, Associated Press* – (Washington; Oregon; Idaho) **Alberstons recalling ground beef in WA, OR.** Albertsons voluntarily recalled a number of ground beef

products sold at its stores in Oregon, Washington, and Idaho, due to risk of E. coli contamination, the Associated Press reported September 24. The move follows an expanded recall by XL Foods Inc. for ground beef products imported to the United States from Canada. The recall includes all of Albertsons stores in Washington and Oregon, as well as three stores in northern Idaho. The products were sold at full service counters and in packaged form with an Albertsons store label between September 3 and September 21. The recall includes the following packaged products with the Albertsons store label: 1-pound fresh ground Beef Patties with the UPC: 7-52907-60030 and use by date of September 11, 1-pound fresh ground beef chub with the UPC: 7-52907-18271 and a use by date of September 18 or 21, and 3-pound fresh ground beef chub with the UPC: 7-52907-18251 and a use by date of September 18 or 21.

Source: <http://www.tri-cityherald.com/2012/09/24/2113106/albertsons-recalling-ground-beef.html#wgt=rcntnews>

25. *September 21, U.S. Food and Drug Administration* – (National) **Maine Natural Health Company issues allergy alert on undeclared allergens in products containing whey protein concentrate.** According to a September 21 release by the U.S. Food and Drug Administration, Maine Natural Health announced a recall of whey protein concentrates. The labels fail to declare the allergens milk, shellfish, and coconut. Affected brands are the Maine Natural Health and Stronger Faster Healthier lines, and include the following products: Pure Whey, Fortified and Endurance Daily, Recovery (also labeled as Post Workout), Rejuvenate, Daily Balance, Endurance Daily, Endurance In Race, and Hunger and Weight. The products were sold in the flavors of chocolate, natural, vanilla, lime, coconut, and pina colada in 2-pound, 10-ounce, and 30-gram sizes. Products were sold from July 14, 2010 through August 31, 2012. They were distributed nationwide directly to consumers via the Internet and through retailers. Source: <http://www.fda.gov/Safety/Recalls/ucm320712.htm>

For another story, see item [3](#)

[\[Return to top\]](#)

Water Sector

26. *September 25, Associated Press; Anchorage Daily News* – (Alaska) **Kenai River's neighbors brace for high water.** The latest round of widespread flooding to hit Southcentral Alaska was aimed at the Kenai Peninsula, the Associated Press reported September 24. The National Weather Service (NWS) extended a flood warning for the Kenai River until September 27. The area included in the warning extends from Kenai Lake to the mouth of the river. At Cooper Landing, the Kenai River was at moderate flood stage September 24. The weather service said that the river would likely continue to rise below Skilak Lake and crest September 25. Residents in low-lying areas, such as the Kenai Keys subdivision near Sterling and the Big Eddy subdivision near Soldotna, were told to prepare for a possible evacuation. The Alaska Department of Natural Resources closed the Kenai River to boat traffic because of dangerously high water September 24. More rain is expected in the area September 25 and September 26, stated the NWS.

Source: <http://www.adn.com/2012/09/24/2638821/kenai-peninsula-braces-for-floods.html>

27. *September 25, Kingston Daily Freeman* – (New York) **Flooding damages Phoenicia backup water supply system.** A torrential downpour resulted in damage to the Phoenicia, New York water supply system and resulted in the declaration of a state of emergency September 18. High water in the Esopus Creek September 18 further eroded a bank that was cut back during Tropic Storm Irene in 2011 and exposed a well casing that is part of the backup system for the Phoenicia water supply. The Phoenicia water commissioner said September 24 that he worries the water district might be left holding the bag. The Federal Emergency Management Agency, he said, had given the district \$150,000 to stabilize the stream bank and protect the well and adjoining pump house after damage to the property during Irene. However, the rainstorm hit before that work could be done. Now that more damage has occurred, it remains unclear what the repair costs will be because the Ulster County Health Department must determine how much of the stream bank needs to be replaced for the well to remain part of the water supply.

Source:

<http://www.dailyfreeman.com/articles/2012/09/25/news/doc506112cee5003262898153.txt>

28. *September 24, Associated Press* – (Arizona) **Boil water alert for Globe residents.** Residents in Globe, Arizona, were asked to boil their water after a city well tested positive for E. coli. City officials said September 24 that the contaminated well is one of six in the area. The well was shut down while further tests were sent to a laboratory. The interim city manager said all water in the city is treated with chlorine. The boil-water mandate was Arizona Department of Environmental Quality protocol. The interim city manager said the results could be caused by many factors including bacteria on one of the testing agent's hands or contaminated testing material. The secondary test results will be available September 25 and if they come back negative for E. coli the city will lift its boil-water alert.

Source: <http://www.kvoa.com/news/boil-water-alert-for-globe-residents/>

29. *September 24, Lexington Herald-Leader* – (Kentucky) **Coal company would pay \$575,000 in water quality reporting lawsuit.** One of Kentucky's largest surface coal-mining companies has agreed to pay \$575,000 in a case that involved thousands of alleged instances of fraudulent or improper water-pollution discharge reports. International Coal Group, or ICG, has reached an agreement in principle with the State and environmental groups to settle claims against the company, stated a status report on the lawsuit the State Energy and Environmental Cabinet filed the week of September 24 in Franklin Circuit Court. The report said ICG would pay Eastern Kentucky Personal Responsibility in a Desirable Environment \$335,000 to rid homes of illegal "straight pipe" sewage discharges, which have fouled water quality in some areas of Eastern Kentucky. ICG also will pay the state \$240,000 to assess the impact of surface mining on waterways.

Source: http://www.hazard-herald.com/view/full_story/20258992/article-Coal-company-would-pay--575-000-in-water-quality-reporting-lawsuit

[\[Return to top\]](#)

Public Health and Healthcare Sector

See item [41](#)

[\[Return to top\]](#)

Government Facilities Sector

30. *September 25, Missouri State University Standard* – (Missouri) **Temple Hall fire caused by chemical reaction.** Cleanup and repair efforts commenced in Temple Hall at Missouri State University in Springfield, Missouri, following a fire that occurred September 19, the Missouri State University Standard reported September 25. According to the director of facilities management, the fire caused damage to adjacent chemistry labs on the fourth floor and was to blame for water damage throughout the building. He said the cause of the fire had to do with a chemical reaction in an experiment being done in a lab in the northeast corner of the building. It was initially thought the sprinklers had been activated, but the facilities manager said the high intensity heat caused a solder joint to let go, causing a 1-inch water line to spew water everywhere. He said the third floor retained the most water, with rooms having 1-2 inches of water in them. The cleanup process involved bringing in heavy-duty equipment including a vacuum to suck up the water, as well as bringing in floor fans and dehumidifiers to dry out the walls.
Source: http://www.the-standard.org/news/temple-hall-fire-caused-by-chemical-reaction/article_7b55efda-06c0-11e2-aa4d-0019bb30f31a.html

31. *September 25, Associated Press* – (Pennsylvania) **Western Pa. community college reopens day after threat to release nerve chemical on campus.** Westmoreland County Community College (WCCC) in Youngwood, Pennsylvania, reopened its campuses a day after receiving threatening phone calls. WCCC officials confirmed the school had reopened September 25. State police from nearby Greensburg were also investigating. County emergency officials said the caller had threatened to release an explosive nerve chemical unless some kind of ransom was paid by 4 p.m. September 24. No dangerous incidents had been reported, however.
Source: <http://www.therepublic.com/view/story/5efe541b4b7341e29aad706dee670e07/PA--Community-College-Threat>

32. *September 24, KJRH 2 Tulsa* – (Oklahoma) **Threat from hacking of city of Tulsa's Web site extends beyond city limits.** The city of Tulsa, Oklahoma's Web site was hacked recently, KJRH 2 Tulsa reported September 24. The potentially compromised data included Social Security, phone, and driver's license numbers. People were notified by letter that their personal information may be in the hands of hackers, thanks to a recent threat to the city of Tulsa's Web site. Officials said the attempt was to access one of the city's computer servers, which hosts the city's Web site. Because the Web site was hacked, officials were urging people whose information was at risk to

place a fraud alert on their information, keep close tabs on credit reports, and consider placing a security freeze on their credit file. The city said those affected submitted an employment application through the city's Web site or reported a crime there. The city's Web site remained down while a criminal investigation continued. Officials said the investigation thus far indicated attempts to access data were "most likely unsuccessful," though the city took the site off-line as a precaution while the investigation was launched. City officials said that they established a resource center to take calls from those who received the letters and have further questions.

Source: http://www.kjrh.com/dpp/news/problem_solvers/threat-from-hacking-of-city-of-tulsa-website-extends-beyond-the-city-limits

33. *September 24, KSWB 5 San Diego* – (California) **Campus library evacuated after pipe bursts.** Students were evacuated from the library at San Diego State University (SDSU) in San Diego, September 24 after a steam pipe burst, campus officials said. The damaged steam pipe caused a major leak at Love Library, according to an SDSU alert system. Power was shut down at the library and nearby Manchester Hall as firefighters worked on the leak. Students and faculty had limited access to the library to retrieve their property. The library would remain closed for the remainder of the evening while repairs were being made, SDSU confirmed.

Source: <http://www.fox5sandiego.com/news/kswb-sdsu-evacuation-pipe-bursts-in-campus-library-20120924,0.5018692.story>

For more stories, see items [36](#) and [41](#)

[\[Return to top\]](#)

Emergency Services Sector

34. *September 25, Las Vegas Sun* – (Nevada) **No one hurt after Metro copter damaged in 'hard landing'.** A Metro Police helicopter on a routine training exercise made a "hard landing" at the North Las Vegas Airport in North Las Vegas, Nevada, September 24, sending two officers to the hospital, officials said. The North Las Vegas Fire Department was called on a report that a helicopter went down, the captain stated. The helicopter attempted to land, but made a "hard landing," a Metro Police spokesman said. Two passengers – a pilot and a second officer – were transported to a nearby hospital to be observed. They suffered no injuries. The North Las Vegas Airport remained open and operational throughout the incident, said a McCarran International Airport spokesman. Investigators from the Federal Aviation Administration and the National Transportation Safety Board were investigating.

Source: <http://www.mynews3.com/content/news/story/Vegas-police-helicopter-damaged-in-hard-landing/-0HEN551qkWF411mwFne4w.csp>

35. *September 24, Associated Press* – (Louisiana) **DOJ seeks to join lawsuit against Orleans prison.** The U.S. Justice Department asked September 24 to join a class-action lawsuit that accuses the Orleans Parish, Louisiana sheriff of overseeing a jail that routinely subjects prisoners to brutal, inhumane conditions. "The Orleans Parish Prison is a violent and dangerous institution," the federal agency said in a request filed in New

Orleans federal court, seeking to be included as a plaintiff in the lawsuit filed by the Southern Poverty Law Center contending the jail's conditions violate the U.S. Constitution. Federal officials have been investigating the Orleans Parish Prison since February 2008, chronicling what they said are repeated instances of jail officials refusing to correct conditions that leave prisoners vulnerable to attacks and rape from other prisoners and their guards. The September 24 court filing says a settlement has been reached to make improvements to prison operations and the settlement will be submitted to the federal judge if the Justice Department is approved to intervene in the case.

Source: http://www.necn.com/09/24/12/DOJ-seeks-to-join-lawsuit-against-Orlean/landing_nation.html?&apID=29732aecdl3742d1871e4a9f403f5c93

36. *September 24, Sierra Vista Herald* – (Arizona) **SE Arizona loses 911 service when line gets cut.** Emergency 9-1-1 service for the entire southeastern corner of Arizona was disrupted for several hours September 24 after a fiber optic cable was severed near Benson. The telephone and DSL cable belonging to CenturyLink was cut causing problems for Graham, Cochise, and Santa Cruz counties, said a market development manager for CenturyLink in southeast Arizona. The incident caused the Cochise County Sheriff's Office and the Sierra Vista Police Department dispatch centers to be overwhelmed by out of area 9-1-1 calls. A Sierra Vista police spokesman said the department's dispatch center received multiple 9-1-1 calls from well outside the normal jurisdiction, including from Mexico. Internet and phone service for county facilities were also disrupted, according to a spokeswoman for the sheriff's office.

Source: <http://www.svherald.com/content/news/2012/09/24/330712>

For more stories, see items [32](#) and [46](#)

[\[Return to top\]](#)

Information Technology Sector

37. *September 25, Softpedia* – (International) **DHL: Most common word used in spear phishing attacks in 2012 H1.** In a new report, FireEye identified a trend in the words being utilized in the names of malicious files sent in spam campaigns. In the second half of 2011, the most common word used in such cybercriminal campaigns was "label." In the first half of 2012, "label" dropped to the 6th position. Currently, the most commonly utilized words in spear phishing attacks are "dhl" and "notification." Each of these words appears in almost a quarter (23.42 percent and 23.37 percent, respectively) of all the malicious attachments that land in users' inboxes. Other words that stand out are "delivery," "express," "2012," "shipment," "ups," "international," "parcel," "post," "confirmation," "alert," "usps," "report," "jan2012," "april," "idnotification," "ticket," and "shipping." This shows that most of the malicious files that come via spam emails are somehow related to shipping. While this may not seem new, the figures from the report reveal that names related to this topic have grown from 19.20 percent to 26.35 percent.

Source: <http://news.softpedia.com/news/DHL-Most-Common-Word-Used-in-Spear-Phishing-Attacks-in-2012-H1-294570.shtml>

38. *September 25, The H* – (International) **Apple fixes security vulnerabilities with Apple TV 5.1 update.** Apple released Update 5.1 for its 2nd and 3rd generation iOS-based Apple TV devices, adding several new features and closing a number of important security holes. According to Apple, Apple TV 5.1 addresses 21 problems, some of which could be exploited by a remote attacker to, for example, cause a denial-of-service (DoS), determine which networks a device previously accessed, or even execute arbitrary code on the device. These include vulnerabilities in the LibXML library used by Apple TV, memory corruption problems in JavaScriptCore and the LibPNG library, a stack buffer overflow in ICU locale ID handling, an integer overflow, a double free bug in ImageIO's handling of JPEG images, and a buffer overflow in the LibTIFF library. For an attack to be successful, a victim must connect to a malicious Wi-Fi network, or open a specially crafted movie or image file.
Source: <http://www.h-online.com/security/news/item/Apples-fixes-security-vulnerabilities-with-Apple-TV-5-1-update-1716561.html>
39. *September 25, Softpedia* – (International) **One billion users affected by Java security sandbox bypass vulnerability, experts say.** Researchers from Security Explorations claimed to identify a flaw that affects all Oracle Java SE versions and the billions of devices on which the software is currently installed. This bug, codenamed issue 50, was identified just before the start of Oracle's JavaOne 2012 conference. "The impact of this issue is critical — we were able to successfully exploit it and achieve a complete Java security sandbox bypass in the environment of Java SE 5, 6 and 7," the CEO of Security Explorations said. He said the vulnerability can be leveraged by an attacker to "violate a fundamental security constraint" of Java Virtual Machines. The researchers confirmed Java SE 5 — Update 22, Java SE 6 — Update 35, and Java SE 7 Update 7 running on fully patched Windows 7 32-bit operating systems are susceptible to the attack. The affected Web browsers are Safari 5.1.7, Opera 12.02, Chrome 21.0.1180.89, Firefox 15.0.1, and Internet Explorer 9.0.8112.16421. The company provided Oracle with a complete technical description of the flaw, along with source and binary codes, and a proof-of-concept that demonstrates the complete security sandbox bypass in Java SE 5, 6, and 7.
Source: <http://news.softpedia.com/news/One-Billion-Users-Affected-by-Java-Security-Sandbox-Bypass-Vulnerability-Experts-Say-294629.shtml>
40. *September 25, The Register* – (International) **A single Web link will wipe Samsung Android smartphones.** A hacker demonstrated how a simple Web page can reset various Samsung phones back to the state they left the factory — enabling a click, bump, or text to take out a victim's mobile device entirely. The flaw lies in Samsung's dialing software, triggered by the tel protocol in a URL. It is not applicable to all the company's Android handsets, but those that are vulnerable can have their PIN changed or be wiped completely just by visiting a Web page or snapping a bad QR code, or even bumping up against the wrong wireless NFC tag.
Source: http://www.theregister.co.uk/2012/09/25/samsung_flaw/
41. *September 25, Nextgov* – (International) **IEEE data breach has global reach.** A Romanian computer programmer currently affiliated with the Computer Science department at the University of Copenhagen, Denmark, claims to have found a log on

the Institute of Electrical and Electronics Engineers's (IEEE) FTP servers containing the log-in information for almost 100,000 of its members. IEEE is one of the world's preeminent professional organizations in such fields as nanotechnology, IT, telecommunications, energy, as well as biomedical and healthcare, and it is a global standards-making organization. According to the programmer, September 18, he first discovered a log with usernames and passwords in plaintext, publicly available via IEEE's FTP server for at least a month. He informed them of his find September 24, and evidently the organization is addressing the issue. Among the users whose information was exposed are researchers at NASA, Stanford, IBM, Google, Apple, Oracle, and Samsung. IEEE's membership of over 340,000 is roughly half American (49.8 percent as of 2011). About 8 percent of IEEE's membership consists of government employees, including the military. Most members work in the private sector and academia.

Source: <http://www.nextgov.com/cybersecurity/cybersecurity-report/2012/09/ieee-data-breach-has-global-implications/58344/>

42. *September 24, Infosecurity* – (International) **Most data breaches come from within.** While the data breach events that catch headlines are the work of hacking collectives and professional malware writers, it turns out that the vast majority of information compromises are caused by companies' own unwitting employees. According to new research from Forrester, only 25 percent of data breach cases are the work of external attackers, and only 12 percent of them were perpetrated by insiders with ill intent. That leaves 63 percent of the issues caused by something more mundane, like losing or misplacing corporate assets, the report found.
Source: <http://www.infosecurity-magazine.com/view/28404/most-data-breaches-come-from-within/>
43. *September 24, Ars Technica* – (International) **Secret Microsoft policy limited Hotmail passwords to 16 characters.** For years, Microsoft engineers quietly limited Hotmail passwords to 16 characters, a revelation that surprised and concerned some users who have long entered passcodes twice that long to access accounts. The limitation is in stark contrast to those found on services such as Gmail, which reportedly permits passwords as long as 200 characters or even Yahoo Mail, which allows 32-character passwords.
Source: <http://arstechnica.com/security/2012/09/secret-microsoft-policy-limited-hotmail-passwords-to-16-characters/>
44. *September 24, PC Magazine* – (International) **New hacker collective emerges in response to anti-Islamic film.** A new, focused group of hackers from a number of Arab countries is reportedly attacking Western Web sites in retaliation for an anti-Islamic video. "The hacking operations are of course a response to the offense against the prophet, peace and blessing be upon him," a member of the self-proclaimed Arab Electronic Army, comprised of hackers from Morocco, Saudi Arabia, Syria, and other countries, told Alarabiya.net recently. So far, the Arab Electronic Army reportedly defaced a number of relatively low-profile Web properties, many of them with Brazilian domain names, according to the spokesman for the hacker collective.
Source: <http://www.pcmag.com/article2/0,2817,2410127,00.asp>

45. *September 24, Threatpost* – (International) **Tiny Evil Maid CHKDSK utility can steal passwords.** Stealthy malware that can sneak onto machines during the boot process and remain undetected indefinitely is one of the ultimate goals of security research. There have been many tools developed over the years that aimed to accomplish this goal, with a researcher's Evil Maid attack being perhaps the most famous. Threatpost reported September 24 that a developer in Canada recently produced a similar tool that impersonates the CHKDSK utility and can grab a user's password and then exit without the user's knowledge. The Evil Maid CHKDSK utility is designed to load from a USB device and will present the user with a screen that looks just like the actual CHKDSK screen, saying the tool is checking the volume on the C: drive for errors.

Source: http://threatpost.com/en_us/blogs/tiny-evil-maid-chkdsk-utility-can-steal-passwords-092412

For more stories, see items [7](#), [8](#), [9](#), [13](#), [32](#), [36](#), and [46](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

46. *September 24, WTVA 9 Tupelo* – (Mississippi) **Phone service down in parts of Calhoun County.** A phone outage plaguing parts of Calhoun County, Mississippi will likely not be resolved for several hours, according to the county's 9-1-1 director. He said someone accidentally cut a fiber optic line near the fire department in Derma September 24. The damage to the line resulted in a loss of landline, ATM, and cell phone coverage for Vardaman and Derma. It also affected the county's 9-1-1 service. Source: <http://www.wtva.com/news/local/story/Phone-service-down-in-parts-of-Calhoun-County/TWgdG5usu0OMp2UrUtMNFg.csp>

For more stories, see items [40](#) and [41](#)

[\[Return to top\]](#)

Commercial Facilities Sector

47. *September 24, Santa Cruz Sentinel* – (California) **Fire guts rooms at National 9 Motel in Watsonville; Fire officials calls cause accidental.** A fire broke out September 24 in a room at National 9 Motel in Watsonville, California, that damaged 7 rooms and displaced 13 people, Watsonville fire officials said. The division chief said the fire appeared accidental and caused by an "open flame." He believed a family of four had rented the room, but they left right after the fire broke out and have not been found. He

estimated the damage at \$250,000 and said 2 of the 7 rooms were severely damaged. Electric lines were burned in the fire and Pacific Gas & Electric was called, fire officials said.

Source: http://www.santacruzsentinel.com/watsonville/ci_21623491/fire-guts-rooms-at-national-9-motel-watsonville?source=most_viewed

48. *September 24, KCRA 3 Sacramento* – (California) **Fire guts 4 Carmichael businesses.** Four Carmichael, California, businesses were gutted by a fire September 24. By the time Sacramento Metro firefighters were called to the business complex, the fire had already spread through most of the building. Despite a two-alarm response, the building suffered serious fire and water damage. Firefighters pulled any items they could salvage from the burning building and used plastic to cover the items they could not move.

Source: <http://www.kcra.com/news/local-news/news-sacramento/Fire-guts-4-Carmichael-businesses/-/12969376/16713504/-/item/0/-/b9ir07z/-/index.html>

49. *September 24, Detroit News* – (Michigan) **Berkley man charged in standoff with police at Royal Oak business.** A suspect has been charged with barricading himself inside a business in Royal Oak, Michigan, with a gun and resisting arrest, Detroit News reported September 24. The Royal Oak police responded to a call of an assault and battery at LGM Landscaping September 21. Family members of the suspect told police there was a physical confrontation between them and the suspect. They said the suspect had a handgun and threatened to kill himself and others. Police heard shots inside the business and secured the area. The Southwest Oakland SWAT Team responded and placed an armored vehicle in front of the business. Following a short standoff, the suspect agreed to leave the building, then struggled with officers during his arrest, police said. He was transported to William Beaumont Hospital for psychiatric evaluation. The suspect was charged with one count of malicious destruction of property, a 4-year felony, and two counts of resisting arrest and obstructing a police officer, a 2-year felony.

Source:

<http://www.detroitnews.com/article/20120924/METRO02/209240433/1361/Berkley-man-charged-in-standoff-with-police-at-Royal-Oak-business>

For more stories, see items [8](#) and [23](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

Nothing to report

[\[Return to top\]](#)

Dams Sector

50. *September 24, WHIO 7 Dayton* – (Ohio) **Bronze from flood gate discovered stolen.** Crews discovered September 24 that control systems on a flood gate in Dayton, Ohio, were stolen. Bronze parts on the storm system, measuring about 15 to 20 feet long, were removed from the gates recently. Police have notified scrap yards to be looking for the parts. The City of Dayton Water Department said the bronze probably weighed about 3 pounds and may be worth about \$1,800.
Source: <http://www.whiotv.com/news/news/bronze-from-flood-gate-discovered-stolen/nSKnG/>
51. *September 24, Manassas News & Messenger* – (Virginia) **Earthquake damage may be causing low water in Lake Jackson.** Damage from the earthquake in August 2011 now may be showing up at the Lake Jackson Dam, in Lake Jackson, Virginia, the Manassas News & Messenger reported September 24. In May, county employees saw that two “toe” drains on the downstream side of the dam were releasing “significant” amounts of water, stated an advisory on the Prince William County Web site. The county said the earthquake may have loosened the seals of “access hatches or low flow hatches/bypasses” allowing water to flow into the interior of the dam. “The preliminary findings of the investigation support this theory, but further investigation is necessary,” the report said. A county contractor performed “exploratory work” on the dam between September 10 and 14 to determine why the drains’ valves were activated and if the excessive water release was causing low water levels in Lake Jackson. Work inspecting the dam was expected to continue for 4 to 6 weeks, stated the advisory. In the meantime, “the whirlpool effect” in the water poses a significant safety hazard and residents were requested to not swim or boat in the area around the dam.
Source: <http://www2.insidenova.com/news/2012/sep/24/earthquake-damage-may-be-causing-low-water-lake-ja-ar-2231203/>

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2273
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes .
Removal from Distribution List:	Send mail to support@govdelivery.com .

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.